UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Richmond Division

JESSICA EASTON, *individually and on behalf of all others similarly situated,*

Plaintiff,

v.

CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., CAPITAL ONE BANK (USA), N.A., AMAZON.COM, INC., and AMAZON WEB SERVICES, INC.,

Defendants.

Case No. 3:19-cv-574

CLASS ACTION COMPLAINT

1. Plaintiff Jessica Easton, individually and on behalf of all others similarly situated (the "Classes"), brings this class action complaint against Defendants Amazon.com, Inc. ("Amazon") and Amazon Web Services ("AWS") (collectively, the "Amazon Defendants") and Capital One Financial Corporation, Capital One, N.A., Capital One Bank (USA) (collectively, the "Capital One Defendants" or "Capital One"). Plaintiff alleges as follows upon personal knowledge as to her own acts and experience, and upon the investigation of her attorneys as to all other matters:

NATURE OF THE ACTION

2. Plaintiff brings this class action lawsuit on her behalf, and on behalf the Classes, against Capital One and the Amazon Defendants for their failure to protect the confidential information of over 100 million consumers including: names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, income, credit scores, credit limits, balances,

payment history, contact information, transaction data, as well as approximately 140,000 social security numbers and approximately 80,000 bank account numbers (collectively "PII").

3. On July 29, 2019, Capital One publicly announced that "there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers." (the "Data Breach").

4. Through its failure to adequately protect Plaintiff's and the Class members' PII, the Amazon Defendants and Capital One allowed Paige A. Thompson ("Thompson"), a former Amazon employee, to obtain access to and to surreptitiously view, remove, and make public Plaintiff's and the Class members' PII entrusted to Capital One, as well as the Amazon Defendants.

5. At all relevant times, Capital One—through its Notice of Privacy Practices and other written assurances—promised to safeguard and protect Plaintiff's and the Class members' PII in accordance with, federal, state and local laws, and industry standards. Capital One breached this promise.

6. Had Capital One informed Plaintiff and Class members that Capital One would use inadequate security measures or entrust their PII to business associates that utilized inadequate security measures, Plaintiff and the Class members would not have provided their PII to Capital One.

7. Capital One's and the Amazon Defendants' failures to implement adequate security protocols jeopardized the PII of millions of consumers, including Plaintiff and the Class members, fell well short of Defendants' promises and obligations, and fell well short of Plaintiff's and other Class members' reasonable expectations for protection of the PII they provided to Capital One who in turn provided such information to Amazon Defendants.

8. As a result of Capital One's conduct and the ensuing Data Breach, Plaintiff and the members of the proposed Classes have suffered actual damages, failed to receive the benefit of their bargains, lost the value of their private data, and are at imminent risk of future harm, including identity theft and fraud which would result in further monetary loss. Accordingly, Plaintiff brings suit, individually and on behalf of the Classes, to seek redress for Defendant's unlawful conduct.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000.00 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists.

10. This Court has personal jurisdiction over the Capital One Defendants because their principal place of business is in this District, and the Capital One Defendants are authorized to and regularly conduct business in this District and Division.

11. This Court has personal jurisdiction over the Amazon Defendants because they are authorized to and regularly conduct business in this District and have sufficient minimum contacts in this District such that the Amazon Defendants intentionally avail themselves of this Court's jurisdiction by conducting operations here, negotiating and providing storage services for the Capital One Defendants headquartered in this District, and promoting, selling and marketing its services to customers in this District.

12. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because the Capital One Defendants' headquarters and principal place of business are located in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by the Capital One Defendants' governance and management personnel or inaction by those individuals that led to

misrepresentations, invasions of privacy and the Data Breach. Moreover, the Capital One Defendants maintain offices in this District and conduct business in this District, and the Amazon Defendants entered into contractual relations with the Capital One Defendants headquartered in this District.

PARTIES

13. Plaintiff Jessica Easton is an individual residing in Easton, Pennsylvania. She applied for and was denied a Capital One credit card in or about April 2019. On information and belief, her PII was compromised in the Data Breach of Capital One's database, which was hosted by the Amazon Defendants. As a result of the Data Breach, Plaintiff Easton has had to carefully review her financial accounts to guard against fraud, failed to receive the benefit of her bargain, lost the value of her private data, and is at imminent risk of future harm, including identity theft and fraud which would result in further monetary loss.

Amazon Defendants

14. Defendant Amazon.com, Inc. is a corporation existing under the laws of the State of Delaware with its headquarters and principal place of business located in the State of Washington at 410 Terry Ave. North, Seattle, WA 98109-5210.

15. Defendant Amazon Web Services, Inc. is a corporation existing under the laws of the State of Delaware with its headquarters and principal place of business located at 410 Terry Ave. North, Seattle, WA 98109-5210. Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc.

Capital One Defendants

16. Defendant Capital One Financial Corporation is a Delaware corporation with its principal place of business located in the Richmond, Virginia region, but its official Headquarters

is listed as McLean, Virginia. Capital One Financial Corp. operates through its two primary subsidiaries, also Defendants here, Capital One Bank (USA) and Capital One, N.A.

17. Capital One Bank (USA), National Association is a subsidiary of Capital One Financial Corporation.

18. Capital One, National Association is a subsidiary of Capital One Financial Corporation.

FACTUAL BACKGROUND

Defendants' Collection and Storage of PII

19. Capital One is a bank holding company specializing in credit cards and offering other credit, including car loans and bank accounts. Capital One offers credit cards and other services to customers throughout the United States. Capital One solicits potential customers to provide them with sensitive PII through applications for credit cards and other financial products.

20. Capital One supports its consumer services, in part, by renting cloud-based storage provided by AWS, where it hosted credit card applications and materials containing customer PII.

21. Cloud computing has boomed as companies have increasingly turned to providers such as Amazon to do the work of configuring computers inside their own data centers. The processing power of those servers and storage devices is then rented out to cloud customers, who pay depending on how much work the computers do.

22. Capital One was an early adopter of cloud-computing among financial institutions, as many other banks hesitated to move sensitive customer data out of their data centers. Capital One started working with AWS in 2014 and has since become a marquee customer. In 2015, Capital One Chief Information Officer Rob Alexander said "the financial services industry attracts some of the worst cybercriminals. So we worked closely with the Amazon team to develop a

security model, which we believe enables us to operate more securely in the public cloud than we can even in our own data centers."

23. According to published reports, the Capital One Defendants here stored Plaintiff's and the Classes' credit card applications containing PII in its cloud computer storage, which was provided by AWS.

24. The Amazon Defendants, through Defendant AWS, provide information technology infrastructure services to businesses like the Capital One Defendants in the form of various web services.[1] AWS offers a range of services, including Amazon Elastic Compute Cloud ("EC2") and Amazon Simple Storage Service ("Amazon S3" or "S3").[2]

25. According to AWS, Amazon S3 "is an object storage service that offers industry-leading scalability, data availability, security, and performance." S3 allows AWS customers to "*store and protect any amount of data*" for a range of use cases, including websites, mobile applications, backup and restore, archive, enterprise applications, Internet of Things ("IoT") devices, and big data analytics. AWS states that S3 provides easy-to-use management features so customers can organize data and configure finely-tuned access controls to meet their specific business, organizational, and compliance requirements.[3]

26. For S3 security, customers only have access to the S3 resources they create. A customer can grant access to other users by using one or a combination of the following access management features: AWS Identity and Access Management ("IAM") to create users and manage their respective access; Access Control Lists ("ACLs") to make individual objects accessible to

[1] *See* Amazon Web Services, https://craft.co/amazon-web-services (last accessed July 31, 2019).
[2] *See* Amazon EC2, https://aws.amazon.com/ec2/ (last accessed July 31, 2019) and Amazon Simple Storage Service, https://aws.amazon.com/s3/ (last accessed July 31, 2019).
[3] *See* Amazon Simple Storage Service, https://aws.amazon.com/s3/ (last accessed July 31, 2019) (emphasis added).

authorized users; bucket policies to configure permissions for all objects within a single S3 bucket; and Query String Authentication to grant time-limited access to others with temporary URLs.[4]

27. AWS notes that "[b]y default, all Amazon S3 resources—buckets, objects, and related subresources . . . are private: only the resource owner, an AWS account that created it, can access the resource."[5]

28. AWS also provides "Amazon GuardDuty" for customers to protect against unwanted threats. AWS declares that "Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads." GuardDuty works by using "machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats." In fact, AWS notes that GuardDuty helps "detect activity such as . . . credential compromise behavior, communication with known command-and-control servers, or API calls from known malicious IPs."[6]

Defendants' Professed Commitment to Data Security

29. AWS makes a public commitment to the security of data stored on its servers:

> At AWS, security is our highest priority. We design our systems with your security and privacy in mind.
>
> - We maintain a wide variety of compliance programs that validate our security controls. . . .
> - We protect the security of your information during transmission to or from AWS websites, applications, products, or services by using encryption protocols and software.
> - We follow the Payment Card Industry Data Security Standard (PCI DSS) when handling credit card data.

[4] *See* Amazon S3 Features, https://aws.amazon.com/s3/features/#Access_management_and_security (last accessed July 31, 2019).
[5] *See* Identity and Access Management, https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html (last accessed July 31, 2019).
[6] *See* Amazon GuardDuty, https://aws.amazon.com/guardduty/ (last accessed August 1, 2019).

- We maintain physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of personal information. Our security procedures mean that we may request proof of identity before we disclose personal information to you.[7]

30. Similarly, the Capital One Defendants promise they are "committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices."[8]

31. Capital One's "Privacy Frequently Asked Questions" states:

> Capital One understands how important security and confidentiality are to our customers, so we use the following security techniques, which comply with or even exceed federal regulatory requirements to protect information about you:
>
> We maintain . . . electronic safeguards, such as passwords and encryption; and procedural safeguards, such as customer authentication procedures to protect against ID theft.
>
> We restrict access to information about you to authorized employees who only obtain that information for business purposes.
>
> We carefully select and monitor the outside companies we hire to perform services for us, such as mail vendors who send out our statements. We require them to keep customer information safe and secure, and we do not allow them to use or share the information for any purpose other than the job they are hired to do.[9]

32. The Frequently Asked Questions web page further states:

> We have taken the following steps to ensure secure Internet services:
>
> We protect our systems and networks with firewall systems.
>
> We employ Intrusion Detection software and monitor for unauthorized access.
>
> We maintain and selectively review activity logs to prevent unauthorized activities from occurring within our computing environment.

---

[7] AWS Privacy Notice, Last Updated: December 10, 2018, https://aws.amazon.com/privacy/ (last visited July 30, 2019).

[8] Capital One Online & Mobile Privacy Statement, https://www.capitalone.com/identity-protection/privacy/statement (last visited July 30, 2019).

[9] *See* Privacy Frequently Asked Questions, https://www.capitalone.com/identity-protection/privacy/faq (emphasis added) (last visited July 30, 2019).

> We use encryption technology to protect certain sensitive information that is transmitted over the Internet.[10]

33. Further, Capital One's "Privacy and Opt Out Notice" stated: "To protect your personal information from unauthorized access and use, **we use security measures that comply with federal law**. These measures include computer safeguards and secured files . . . ."[11]

34. Similarly, Capital One's "Social Security Number Protections" disclosure stated:

> Capital One protects your Social Security Number. Our policies and procedures: 1) Protect the confidentiality of Social Security numbers; 2) Prohibit the unlawful disclosure of Social Security numbers; and 3) Limit access to Social Security numbers to employees or others with legitimate business purposes.
>
> These safeguards apply to all Social Security numbers collected through any channel or retained in any way by Capital One in connection with customer, employee or other relationships.[12]

35. Unfortunately for Plaintiff and the Classes, Defendants failed to live up to these explicit, as well as other implicit promises about the security of customer PII.

The Capital One Data Breach

36. On July 29, 2019, Capital One announced that the PII of more than 100 million individuals had been compromised.[13]

37. According to Capital One, the Data Breach compromised "information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019," and included "names, addresses, zip codes/postal codes, phone

---

[10] *Id.* (emphasis added).
[11] *See* Capital One Privacy Notice, https://www.capitalone.com/privacy/notice/en-us/ (emphasis added) (last visited July 31, 2019).
[12] *See* Social Security Number Protections, https://www.capitalone.com/identity-protection/privacy/social-security-number (emphasis added) (last visited July 31, 2019).
[13] Press Release, Capital One (July 29, 2019), https://www.capitalone.com/facts2019/

numbers, email addresses, dates of birth, . . . self-reported income[,] . . . credit scores, credit limits, balances, payment history, contact information" and "transaction data."[14]

38. Capital One also disclosed that the Data Breach compromised the social security numbers of approximately 140,000 of the bank's credit card customers, and the bank account numbers of approximately 80,000 of the bank's secured credit card customers.[15]

39. The Data Breach was executed by Paige Thompson (a/k/a "erratic"), a former "systems engineer" for Amazon. On July 29, 2019, the FBI arrested, and federal prosecutors charged, Thompson in the United States District Court for the Western District of Washington with computer fraud and abuse in violation of 18 U.S.C. § 1030(a)(2).

40. Because Thompson is a former employee at Amazon's web services unit, the world's biggest cloud-computing business, that raises questions about whether she used knowledge acquired while working at the cloud-computing giant to commit her alleged crime, said Chris Vickery director of cyber-risk research at the security firm UpGuard Inc.

41. According to the criminal complaint, Thompson was able to gain access to PII collected by Capital One and stored on Capital One and AWS' systems. Thompson exploited a "configuration vulnerability" to gain access to the systems.[16] According to Capital One, this "unauthorized access also enabled the decrypting of data."[17]

42. Published reports suggest that the attacker exploited a type of vulnerability known as Server-Side Request Forgery (SSRF) to perform the attack.[18] By exploiting an SSRF

---

[14] *Id.*
[15] *Id.*
[16] Frequently Asked Questions, Capital One (July 31, 2019), https://www.capitalone.com/facts2019/2/.
[17] *Id.*
[18] *See* Early Lessons from the Capital One Data Breach, Stratum Security (July 31, 2019) https://blog.stratumsecurity.com/2019/07/31/early-lessons-from-the-capital-one-breach/ (last accessed August 1, 2019).

vulnerability, an attacker can trick a server into disclosing sensitive server-side information that would otherwise be inaccessible outside the firewall.[19] In this case, reports suggest that Thompson was able to use SSRF to execute a request on an AWS EC2 instance controlled by Capital One that revealed Capital One's S3 credentials.[20]

43. This attack was possible due to a ***known*** vulnerability in AWS, that Amazon Defendants have failed to correct, that allows SSRF attackers to trick AWS EC2 instances into disclosing an AWS users' credentials.[21] The single-line command that exposes AWS credentials on any EC2 system is known by AWS and is in fact included in their online documentation.[22] It is also well known among hackers.

44. SSRF is a known vulnerability and Amazon Defendants have done nothing to fix it.

45. Thompson initially gained access to Capital One's systems on March 22, 2019, and the breach continued through at least April 21, 2019.[23]

46. In a June 16, 2019 tweet, Thompson described a method for gaining access to files stored on AWS S3 systems that appears to closely match the method used to access Capital One's data:

---

[19] Id.
[20] Id.
[21] Id.
[22] *See* IAM Roles for Amazon EC2 *https*://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html (last accessed August 1, 2019).
[23] *Id.*

47. Notably, the attack vector described by Thompson in her June 16, 2019 tweet **is not limited to Capital One's systems**. Rather, it exploits a general vulnerability of certain configurations of AWS S3 systems in general using a widely known vulnerability of which the Amazon Defendants were aware and could have prevented.

48. In fact, Thompson was apparently able to take advantage of this AWS configuration vulnerability to breach a number of other large corporations and organizations through the AWS network, including "one of the world's biggest telecom providers, an Ohio government body and a major U.S. university."[24]

49. The FBI has confirmed that it is examining whether Thompson hit other targets like Michigan State, the Ohio Department of Transportation, UniCredit SpA (Italy's largest bank), and

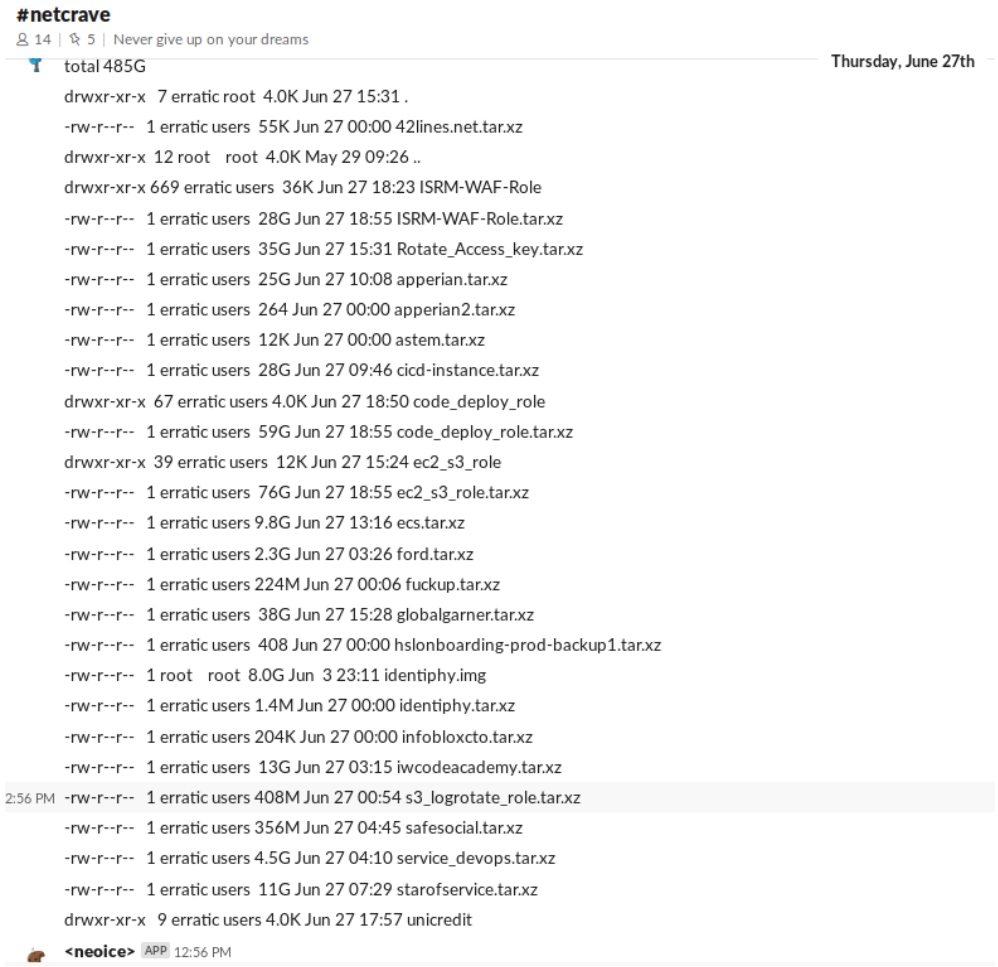
[24] *See* Thomas Brewster, *DOJ Says Capital One Mega Breach Suspect Could Face More Charges—Did She Hack Multiple Companies?*, Forbes (July 30, 2019), https://www.forbes.com/sites/thomasbrewster/2019/07/30/capital-one-mega-breach-suspect-may-have-hacked-many-more-companies (last accessed July 31, 2019); *see also* Paige A. Thompson Criminal Complaint, Case No. MJ19-0344 ¶ 25 (W.D. Wash.) ("I understand this post to indicate, among other things, that PAIGE A. THOMPSON intended to disseminate data from *victim entities, starting with Capital One*.") (emphasis added).

Ford. As the *Wall Street Journal* reported, "the widening probe points up a possible weakness: A hacker who figures out a way around the security fence of one cloud customer not only gets to that customer's data but also has a method that might be usable against others."[25]

50. Thompson further posted a comment in a public chatroom on the chat platform Slack on June 27, 2019, listing various databases of companies and organizations she found while hacking the AWS cloud instances in the manner described above.[26] The following is a screenshot of Thompson's Slack comment, which includes names of a number of large companies and organizations:

[25] Anuj Gangahar and Dana Mattioli, *FBI Examining Possible Data Breaches Related to Capital One*, Wall Street Journal (July 31, 2019), https://www.wsj.com/articles/italys-unicredit-investigating-data-breach-possibly-related-to-capital-one-11564587592 (last accessed July 31, 2019).

[26] *See* Brian Krebs, *Capital One Data Theft Impacts 106M People*, Krebs On Security, https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/ (last accessed July 31, 2019).



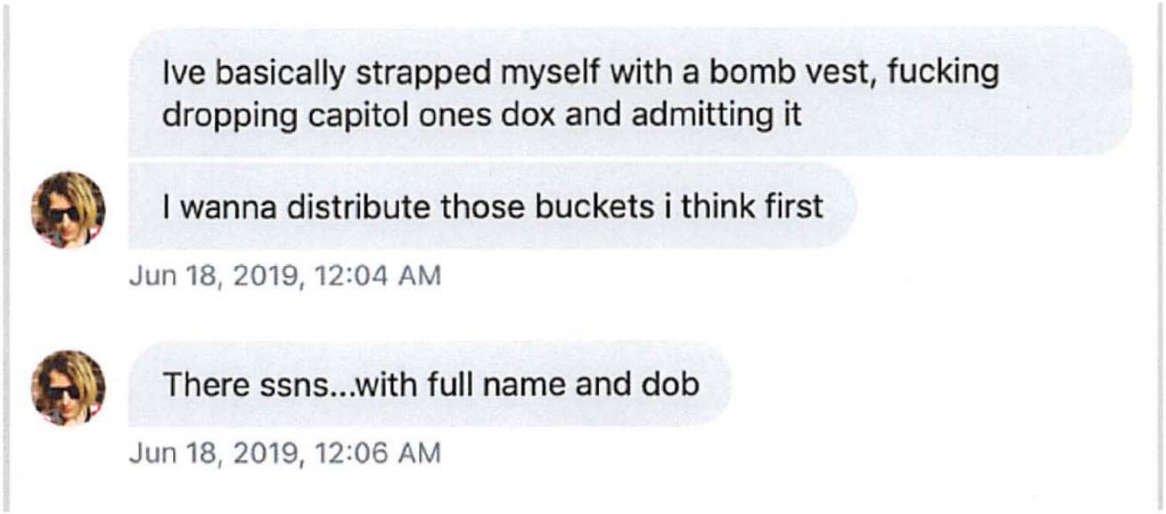
51. Despite these public boasts, Defendants did not discover the breach until four months after Thompson initially gained access to the breached data through the AWS configuration vulnerability, when an unknown third party emailed the Capital One Defendants on July 17, 2019.[27]

Dissemination of Breached Data

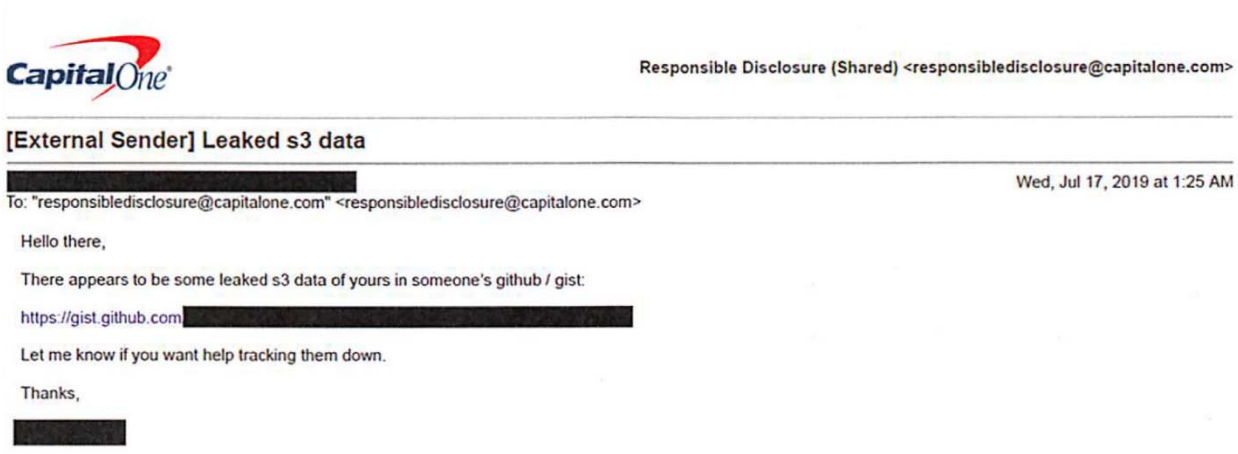
52. According to the criminal complaint, Thompson "intended to disseminate data stolen from victim entities, starting with Capital One."[28] As shown in the image below from the

[27] https://www.capitalone.com/facts2019/
[28] Thompson Criminal Complaint, at 12.

criminal complaint, Thompson stated that "I wanna distribute those buckets," and noted that the Capital One data included "ssns...with full name and dob."[29]



53. It appears that Thompson succeeded in disseminating the hacked information. According to the third party who notified Capital One of the Data Breach, some of the bank's internal data, which had been stored on the AWS S3 platform, had been posted publicly on the code-sharing and easily accessible website GitHub. [30]



[29] *Id.* at 11–12.
[30] *Id.* at 5–6.

54. The GitHub page referenced by the third party also included executable code, which Capital One confirmed "function[d] to obtain Capital One's credentials, to list or enumerate folders or buckets of data, and to extract data from certain of those folder or buckets."[31]

55. It's not yet clear how many other hackers or individuals may have downloaded Capital One's data or exploited its credentials.

56. Capital One said it expected to spend up to $150 million to cover breach-related costs, largely for issues such as notifying customers and paying for credit monitoring. The bank has discussed potential fines or reimbursement to consumers.

Data Security Breaches Lead to Increased Actual and Potential Identity Theft.

57. Defendants knew or should have known that the PII that they were collecting from Plaintiff and Class members, which was stolen during the Data Breach, was highly valuable and highly sought-after by criminals.

58. There has been an "upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published."[32]

59. The United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report") that identity thieves use personally identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[33] As the GAO Report notes, this type of identity theft is the most harmful because it may take some

[31] *Id*. at 7.
[32] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited July 31, 2019).
[33] *See* United States Government Accountability Office, *Personal Information: Data Breaches Are Frequent, But Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf.

time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

60. In addition, the GAO Report makes clear that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[34]

61. Identity theft victims must often spend countless hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[35]

62. With access to an individual's PII, criminals can do more than just empty a victim's bank account; they can also commit many types of fraud, including: obtaining a driver's license or other official identification card in the victim's name but with the thief's picture on it; using the victim's name and social security number to obtain government benefits; and filing a fraudulent tax return using the victim's PII. In addition, identity thieves may obtain a job using the victim's PII, rent a house or receive medical services, prescription drugs and goods, and cause fraudulent medical bills to be issued in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued against the

[34] *Id*.

[35] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

identity theft victim.[36] Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail and other negative effects.

63. PII is a valuable commodity to identity thieves. Compromised PII is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers, and other PII directly on various dark web[37] sites making the information publicly available.[38]

CLASS ACTION ALLEGATIONS

64. Plaintiff brings this action individually and on behalf of all others similarly situated as a class action under Federal Rules of Civil Procedure 23, seeking damages and equitable relief on behalf of the following nationwide Class ("Class", to include both subclasses) for which Plaintiff seeks certification:

> All natural persons residing in the United States and whose PII was disclosed in the Data Breach.

65. Excluded from the Class are employees of Capital One; any parent, affiliate, or subsidiary of Capital One; employees of any entity in which Capital One has a controlling interest; any of Capital One's officers or directors; or any successor or assign of Capital One. Also excluded are any Judge or court personnel assigned to this case and Members of their immediate families,

---

[36] *See Warning Signs of Identity Theft*, Federal Trade Commission, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 31, 2019).

[37] The dark web refers to online content that cannot be found using conventional search engines and can be accessed only through specific browsers and software. MacKenzie Sigalos, *The Dark Web and How to Access It*, CNBC (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last accessed July 31, 2019).

[38] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian Blog (Mar. 11, 2019), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited July 31, 2019); McFarland et al., *The Hidden Data Economy* 3, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last visited July 31, 2019).

all attorneys representing the Plaintiff and any employees or immediate family members of such attorneys.

66. **Numerosity. Fed. R. Civ. P. 23(a)(l).** The Class is so numerous that joinder of all Members is impracticable. While Plaintiff does not know the exact number of the Members of the Class, Plaintiff believes the Class contains approximately 100 million people. Class Members may be identified through objective means using Capital One's records. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media, and/or published notice.

67. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** This action involves common questions of law and fact exist as to all Members of the Class, and predominate over any questions affecting individual Members of the Class. Such questions of law and fact common to the Class include, but are not limited to:

a. Whether Capital One had a duty to adequately protect PII from consumers who applied for Capital One credit card products;

b. Whether Capital One breached that duty by acts or omissions;

c. Whether the breach proximately caused damages to Plaintiff and Class Members;

d. Whether and when Capital One knew or should have known of the susceptibility of its computer systems to a data breach;

e. Whether Capital One's security measures to protect its computer systems were reasonable in light of the FTC data security recommendations and best practices recommended by data security experts;

f. Whether Capital One was negligent in failing to implement reasonable and adequate security procedures and practices to protect the information it collected and stored from consumers who applied for Capital One credit card products;

g. Whether Capital One's conduct, practices, actions, and/or omissions constituted unfair or deceptive trade practices;

h. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Capital One's failure to reasonably protect its computer systems and data network; and

i. The relief, including injunctive relief, to which Plaintiff and Class Members are entitled.

68. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiff's claims are typical of the claims of the Members of the Class. Plaintiff is a consumer who provided PII to in order to apply for Capital One credit card products and had their PII compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with the relief of the Class Members.

69. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiff is an adequate representative of the Class because Plaintiff is a Member of the Class and are committed to pursuing this matter against Capital One to obtain relief for the Class. Plaintiff has no conflicts of interest with Class Members. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests. Plaintiff's claims arise out of the same common course of conduct giving rise to the claims of the other Members of the Class. Plaintiff's interests are coincident with, and not antagonistic to, those of the other Members of the Class.

70. **Superiority. Fed. R. Civ. P. 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no difficulties exist that are likely to impact the management of this class action. The quintessential purpose of the class action device is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Capital One, and thus, individual litigation to redress

Capital One's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system because of the millions of cases that would need to be filed and litigated. Individual litigation also creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action mechanism presents far fewer management difficulties and provides the benefits of a single adjudication using common proof and before a single court.

71. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Capital One, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate for the Class.

72. Similarly, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues are set forth in Paragraphs 1 through 118 above.

73. Finally, all Members of the proposed Class are readily ascertainable. Capital One has access to information regarding the applications from consumers for the span of time from 2005 through 2019 and the consumers affected by the Data Breach. Using this information, Class Members can be identified, and their contact information ascertained for the purpose of providing notice to the Class. The national consumer reporting agencies, Capital One and other available sources retain information sufficient to identify individuals who were victims of Identity Theft and did not in fact apply for the subject Capital One product.

FIRST CLAIM FOR RELIEF
Negligence (For the Class)

74. Plaintiff restates and realleges the above paragraphs as if fully set forth herein.

75. Capital One demanded and took possession of Plaintiff's and the Class Members' PII, meaning Capital One then had a duty to exercise reasonable care in protecting that information from unauthorized access or disclosure. Capital One further had a duty to destroy Plaintiff's and Class Members' PII within an appropriate amount of time after it was no longer required by Capital One, in order to mitigate the risk of such stale PII being compromised in the Data Breach.

76. Upon accepting and storing Plaintiff's and Class Members' PII in its computer systems and networks, Capital One undertook and owed a duty of care to Plaintiff and Class Members to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII and to use commercially-reasonable methods to do so. Capital One knew that the PII was private, personal, and confidential, and should be protected.

77. Capital One owed a duty of care not to subject Plaintiff and Class Members, along with their PII, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

78. Capital One owed a duty of care to Plaintiff and Class Members to quickly detect a data breach and to timely act on warnings about data breaches.

79. These duties arose from Capital One's relationship to Plaintiff and Class Members and from industry custom.

80. Capital One, through its actions and inactions, unlawfully breached duties to Plaintiff and Class Members by failing to implement standard industry protocols and to exercise reasonable care to secure and keep private the PII entrusted to it.

81. Capital One, through its actions and omissions, allowed unmonitored and unrestricted access to unsecured PII.

82. Through its actions and omissions, Capital One failed to provide adequate supervision and oversight of the PII with which it was entrusted, despite knowing the risk and foreseeable likelihood of a breach and misuse, which permitted unknown third parties to gather Plaintiff's and Class Members' PII, misuse that PII, and intentionally disclose it to unauthorized third parties without consent.

83. Capital One knew or should have known the risks inherent in collecting and storing PII, the importance of adequate security and the well-publicized data breaches within the financial services industry.

84. Capital One knew or should have known that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

85. Due to Capital One's knowledge that a breach of its systems would damage millions of its customers like Plaintiff and Class Members, Capital One had a duty to adequately protect its data systems and the PII contained thereon.

86. Capital One had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Capital One with their PII was predicated on the understanding that Capital One demanded the PII and therefore would take adequate security precautions to safeguard that information. Moreover, only Capital One had the ability to protect its systems and the PII stored on those systems from attack.

87. Capital One's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII. Capital One's misconduct included failing to: (1) secure its computer systems, despite knowing their vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

88. Capital One also had independent duties under federal laws that required Capital One to reasonably safeguard Plaintiff's and Class Members' PII, and promptly notify them about the Data Breach.

89. Capital One breached its duties to Plaintiff and Class Members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Customer Data;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' PII before and after learning of the Data Breach;

d. by failing to comply with industry standard data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiff and Class Members' PII had been improperly acquired or accessed.

90. Through Capital One's acts and omissions described in this Complaint, including Capital One's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Capital One unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' PII while it was within Capital One's possession or control.

91. The law further imposes an affirmative duty on Capital One to timely disclose the unauthorized access and theft of Plaintiff's and Class Members' PII, so that Plaintiff and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

92. Capital One breached its duty to notify Plaintiff and Class Members of the unauthorized access to their PII by waiting to notify Plaintiff and Class Members, and then by failing to provide Plaintiff and Class Members sufficient information regarding the breach.

93. Through Capital One's acts and omissions described in this Complaint, including Capital One's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Capital One unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' PII while it was within Capital One's possession or control.

94. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Capital One prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

95. Upon information and belief, Capital One improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Capital One's failure to take proper security measures to protect sensitive PII as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' PII.

96. Capital One's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class Members' PII; and failing to provide Plaintiff and Class Members with timely and sufficient notice that their sensitive PII had been compromised.

97. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint

98. Capital One's failure to exercise reasonable care in safeguarding PII by adopting appropriate security measures, including proper encryption storage techniques, was the direct and proximate cause of Plaintiff's and Class Members' PII being accessed and stolen through the data breach.

99. Capital One breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

100. As a result of Capital One's breach of duties, Plaintiff and the Class suffered damages including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

SECOND CLAIM FOR RELIEF
Negligence *Per Se* (For Class)

101. Plaintiff restates and realleges the above paragraphs as if fully set forth herein.

102. Section 5 of the FTC Act prohibits ''unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Capital One, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Capital One's duty in this regard.

103. Capital One violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII, and not complying with applicable industry standards, as described in detail herein. Capital One's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the immense damages that would result to Plaintiff and Class Members.

104. Capital One's violation of Section 5 of the FTC Act constitutes negligence *per se.*

105. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

106. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

107. As a direct and proximate result of Capital One's negligence *per se,* Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia,* by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

108. Additionally, as a direct and proximate result of Capital One's negligence *per se,* Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Capital One's possession and is subject to further unauthorized disclosures so long as Capital One fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract (For the Class)

109. Plaintiff restates and realleges the above paragraphs as if fully set forth herein.

110. Capital One solicited Plaintiff and Class Members to apply for credit card products and demanded their PII in that process. Providing PII to Capital One was a condition for Plaintiff and Class Members to receive credit. Plaintiff and Class Members accepted Capital One's offers and provided their PII to Capital One to apply for Capital One credit card products.

111. When Plaintiff and Class Members applied for Capital One credit card products, they provided their PII to Capital One as a prerequisite to obtaining credit. In so doing, Plaintiff and Class Members on the one hand, and Capital One on the other, entered into mutually agreed-upon implied contracts pursuant to which Plaintiff and Class Members agreed that their PII was valid, while Capital One agreed that it would use Plaintiff and Class Members' PII in its possession for only the agreed-upon purpose of processing the credit card product applications, and no other purpose.

112. Implicit in the agreement to use the PII in its possession for only the agreed-upon application and no other purpose was the obligation that Capital One would use reasonable measures to safeguard and protect the PII of Plaintiff and Class Members in its possession.

113. By accepting PII for credit card product applications, Capital One assented to and confirmed its agreement to reasonably safeguard and protect Plaintiff's and Class Members' PII

from unauthorized disclosure or uses and to timely and accurately notify Plaintiff and Class Members if their data had been breached and/or compromised.

114. Plaintiff and Class Members would not have provided and entrusted their PII to Capital One to apply for the Capital One credit card products in the absence of this implied contract between them and Capital One.

115. Plaintiff and Class Members fully performed their obligations under the implied contracts with Capital One.

116. Capital One breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect Plaintiff's and Class Members' PII, and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

117. Capital One breached the implied contracts it made with Plaintiff and Class Members by failing to ensure that Plaintiff's and Class Members' PII in its possession was used only for the agreed-upon application verification and no other purpose.

118. Plaintiff and Class Members conferred a monetary benefit on Capital One which has accepted or retained that benefit. Specifically, the credit card products typically carry annual fees and other charges (e.g. interest) for use. In exchange, Plaintiff and Class Members should have received the services that were the subject of the transaction and should have been entitled to have Capital One protect their PII with adequate data security measures.

119. Capital One failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

120. Capital One acquired the PII through inequitable means when it failed to disclose the inadequate security practices previously alleged.

121. If Plaintiff and Class Members had known that Capital One would employ inadequate security measures to safeguard PII, they would not have applied for the Capital One credit card products or otherwise shared their PII with Capital One.

122. As a direct and proximate result of Capital One's breaches of the implied contracts between Capital One on the one hand, and Plaintiff and Class Members on the other, Plaintiff and Class Members sustained actual losses and damages as described in detail above.

123. Plaintiff and Class Members were harmed as the result of Capital One's breach of the implied contracts because their PII was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the dark web. Plaintiff and the Class have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, late fees, bank fees, and other expenses relating to identity theft losses or protective measures. The Class Members are further damaged as their PII remains in the hands of those who obtained it without their consent.

124. This breach of implied contracts was a direct and legal cause of the injuries and damages to Plaintiff and Class Members as described above.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment (For the Class)

125. Plaintiff restates and realleges the above paragraphs as if fully set forth herein.

126. Plaintiff and Members of the Class conferred a monetary benefit on Capital One. Specifically, they provided and entrusted their PII to Capital One.

127. In exchange, Plaintiff and Class Members should have been entitled to have Capital One protect their PII with adequate data security.

128. Capital One appreciated, accepted, and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Capital One's conduct toward Plaintiff and Class Members as described herein; Plaintiff and Class Members conferred a benefit on Capital One and accepted or retained that benefit. Capital One used Plaintiff's and Class Members' PII for business purposes.

129. Capital One failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

130. Capital One acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged, as well as failing to destroy or otherwise purge the PII from its computer systems after Capital One no longer had a legitimate business purpose to maintain that PII.

131. If Plaintiff and Class Members knew that Capital One would not secure their PII using adequate security, they would not have applied for Capital One credit card products.

132. Plaintiff and Class Members have no adequate remedy at law for the injuries they suffered due to Capital One's conduct.

133. Under the circumstances, it would be unjust for Capital One to be permitted to retain any of the benefits that Plaintiff and Class Members conferred on it.

134. Under the principles of equity and good conscience, Capital One should not be permitted to retain the PII belonging to Plaintiff and Class Members because Capital One failed to implement the data management and security measures that industry standards mandate.

135. Capital One should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

In the alternative, Capital One should be compelled to refund the amounts that Plaintiff and Class Members overpaid for security they did not receive.

FIFTH CLAIM FOR RELIEF
Declaratory Judgment (For the Class)

136. Plaintiff restates and realleges the above paragraphs as if fully set forth herein.

137. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Capital One to provide adequate security for the PII it collected from their applications for Capital One credit card products. As previously alleged, Capital One owes duties of care to Plaintiff and Class Members that require it to adequately secure PII.

138. Capital One still possesses PII pertaining to Plaintiff and Class Members.

139. Capital One has not announced or otherwise notified Plaintiff and Class Members that their PII are sufficiently protected or, more importantly, expunged from Capital One's servers so as to prevent any further breaches or compromises.

140. Indeed, Capital One has stated that PII from Capital One credit card product applications submitted as far back as 2005 is subject to the Data Breach.

141. Accordingly, Capital One has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Capital One's lax approach to data security has become public, the PII in its possession is more vulnerable than before.

142. Actual harm has arisen in the wake of the Data Breach regarding Capital One's contractual obligations and duties of care to provide data security measures to Plaintiff and Class Members.

143. Plaintiff therefore seeks a declaration that: (a) Capital One's existing data security measures do not comply with its contractual obligations and duties of care; and (b) in order to

comply with its contractual obligations and duties of care, Capital One must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Capital One's systems on a periodic basis, and ordering Capital One to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Capital One is compromised, hackers cannot gain access to other portions of Capital One's systems;

e. purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

f. conducting regular database scans and security checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Capital One's customers should take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully seeks from the Court the following relief:

a. Certification of the Class as requested herein under Federal Rule of Civil Procedure 23;

b. Appointment of Plaintiff as Class Representative and her undersigned Counsel as Class counsel;

c. Award Plaintiff and Members of the proposed Class damages;

d. Award Plaintiff and Members of the proposed Class equitable, injunctive and declaratory relief, including the enjoining of Capital One's insufficient data protection practices at issue herein and Capital One's continuation of its unlawful business practices as alleged herein;

e. An order declaring that Capital One's acts and practices with respect to the safekeeping of PII were negligent;

f. Award Plaintiff and Members of the proposed Class pre-judgment and post-judgment interest as permitted by law;

g. Award Plaintiff and Members of the proposed Class reasonable attorneys' fees and costs of suit, including expert witness fees; and

h. Award Plaintiff and Members of the proposed Class any further relief the Court deems proper.

TRIAL BY JURY IS HEREBY DEMANDED.

Dated: August 9, 2019

Respectfully submitted,

PLAINTIFFS,

By: /s/
Scott A. Surovell
Email: ssurovell@surovellfirm.com
SUROVELL ISAACS & LEVY PLC
4010 University Drive, Suite 200
Fairfax, VA 22030
Tel: (703) 277-9750
Fax: (703) 591-9285

Shanon J. Carson
Email: scarson@bm.net
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel.: (215) 875-3000
Fax: (215) 875-4604

E. Michelle Drake
Email: emdrake@bm.net
BERGER MONTAGUE, PC
43 SE Main Street, Suite 505
Minneapolis, MN 55414
Tel: (612) 594-5933
Fax: (612) 584-4470

Attorneys for Plaintiff and Proposed Class